(19) Europäisches Petentamt
European Patent Office
Office européen des brevete

(11) EP 0 388 131 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
06.03.1996 Bulletin 1996/10

(51) Int Cl.[6]: **G06F 7/58**

(21) Application number: **90302630.0**

(22) Date of filing: **13.03.1990**

(54) Random number generator

Zufallszahlengenerator

Générateur de nombres aléatoires

(84) Designated Contracting States:
DE FR GB

(30) Priority: **15.03.1989 JP 62562/89**

(43) Date of publication of application:
19.09.1990 Bulletin 1990/38

(73) Proprietor: **Oki Electric Industry Co., Ltd.**
Tokyo (JP)

(72) Inventor: **Tanagawa, Kouji,**
c/o Oki Electric Ind. Co. Ltd.
Tokyo (JP)

(74) Representative: **Read, Matthew Charles et al**
Venner Shipley & Co.
20 Little Britain
London EC1A 7DH (GB)

(56) References cited:
FR-A- 2 375 824 **US-A- 4 665 502**

- **IBM TECHNICAL DISCLOSURE BULLETIN. vol. 28, no. 6, November 1985, NEW YORK US pagee 2303 - 2304; "NON-REPETITIVE RANDOM SEQUENCER"**
- **PATENT ABSTRACTS OF JAPAN vol. 10, no. 371 (P-526)(2428) 11 December 1986, & JP-A-61 163435 (MATSUSHITA ELECTRIC WORKS LTD) 24 July 1986**
- **PATENT ABSTRACTS OF JAPAN vol. 6, no. 41 (P-106)(919) 13 March 1982, & JP-A-56 157535 (SHARP K.K.) 04 December 1981**
- **PATENT ABSTRACTS OF JAPAN vol. 11, no. 292 (E-543)(2739) 19 September 1987, & JP-A-62 091039 (FUJITSU LTD) 25 April 1987**

EP 0 388 131 B1

Printed by Jouve, 75001 PARIS (FR)

Description

The present invention relates to a data processing integrated circuit including a random number generator.

Many integrated circuits such as single-chip microcomputers require built-in random number generators for purposes such as coding and decoding data. In many cases very large random numbers are required, comprising many digits or bits, which must be assembled from a series of successively generated random numbers. A random number generator should therefore be capable of generating successive random numbers quickly, but it should not require extensive circuitry, since space in an integrated circuit is limited.

One prior-art random number generator comprises an arithmetic unit that repetitively performs certain arithmetic operations, the results of which are kept in a decimal counter. Random numbers are requested by key input by a human operator. When such input occurs, the arithmetic operations are halted and the current counter contents are output as a random number. This random number generator, however, requires extensive counter and arithmetic circuitry, and needs several seconds to generate a random number with a large number of digits.

Another prior-art random number generator uses logic gates and an M-series pseudo-random number generator, for example, to generate a group of clock pulses with differing pulse counts. The clock pulses are counted by a counter, and the counter output is used as a pseudo-random number. This random number generator, however, also requires extensive circuitry and cannot generate random numbers at a rapid rate.

Yet another prior-art random number generator uses a plurality of small-capacity read-only memories from which data are read at independent cycles, and generates longperiod pseudo-random numbers by performing arithmetic operations on the data read from the read-only memories. This random number generator, however, is limited in speed by the time needed for performing the arithmetic operations, and requires extensive memory circuitry if it is to generate large random numbers.

A further random number generator, wherein numbers from two pseudo-random number generators are combined to produce an output random number, is known from "IBM Technical Disclosure Bulletin", Vol. 28, No. 6, November 1985.

Also, JP-A-61-163435 discloses a random number generator comprising a counter and a RAM. When a random number is requested, the current value of the counter is stored in the RAM and an arithmetic unit either reads the stored low order bits or reads and transposes the stored high and low order bits, depending on the size of the random number required.

An object of the present invention is accordingly to generate successive random numbers quickly,

Another object is to generate random numbers with simple circuitry.

According to the present invention, there is provided a data processing integrated circuit comprising data processing circuitry including a system bus and a system clock, and a random number generator, wherein the random number generator comprises oscillator means arranged to produce clock pulse signals independent of the system clock, a plurality of counters arranged to generate numbers by counting the clock pulse signals and read out means responsive to a read signal from the processing circuitry to apply the counter contents directly to the system bus.

Preferably, the oscillator means comprises a plurality of independent oscillators.

Preferably, the random number generator further comprises an AND gate, connected between said oscillator means and said counter for gating the said clock pulse signals in response to the read signal, and a read-out control circuit disposed in each of the counters for outputting the contents of the respective counters in response to the read signal.

Preferably, the integrated circuit includes read-out means for causing the counters to stop counting while their contents are applied to the system bus.

Embodiments of the present invention will now be described, by way of example, with reference to the accompanying drawings, in which:

Fig. 1 is a schematic diagram illustrating a novel random number generator;
Fig. 2 is a timing chart illustrating the operation of the random number generator in Fig. 1; and
Fig. 3 is a schematic diagram illustrating another novel random number generator.

Two random number generators embodying the present invention will be described with reference to Figs. 1 and 3. Both random number generators are shown as delivering 16-bit random numbers to a system bus in an integrated circuit such as a single-chip microcomputer, of which most part of the random number generator is a component. The integrated circuit is driven by a system clock, not explicitly shown in the drawings, and requests random numbers by driving a read signal to the high (active) state at times controlled, for example, by a microcomputer application program.

The random number generator shown in Fig. 1 is provided with a pair of oscillators 1 and 2, which may be RC oscillators or crystal oscillators, for generating clocks pulses CP1 and CP2. When crystal oscillators are employed, the crystals (quartz) are provided outside of the integrated circuit and connected to the integrated circuit. The clock pulses CP1 and CP2 are mutually independent, meaning that they are asynchronous, and both are independent of the system clock.

The clock pulses CP1 and CP2 are gated by AND gates 3 and 4 and counted by a pair of counters 5 and 6. More specifically, the AND gate 3 receives the clock pulses CP1 and the inverse of the read signal (RD) as inputs, performs a logical AND operation on these inputs,

and provides the result as output to the clock (CK) terminal of the counter 5. Similarly, the AND gate 4 ANDs the clock pulses CP2 with the inverse of the read signal and provides the result to the clock terminal of the counter 6. The counters 5 and 6 count the pulses received at their clock terminals.

The counters 5 and 6 in Fig. 1 are eight-bit up-counters, the contents of which are output at output terminals Q1, Q2, ..., Q8 and Q9, Q10, ..., Q16, respectively. The counter 5 includes a read-out control circuit 7 which outputs the counter contents at Q1 to Q8 only when a high signal is received at an output enable (OE) terminal, to which the read signal is connected. When the read signal is low, Q1 to Q8 are kept in the high-impedance state. The counter 6 includes a similar read-out control circuit 8 that outputs Q9 to Q16 only when a high read signal is received.

The output terminals Q1 to 16 are connected to a 16-bit system bus 9 which carries the outputs Q1 to Q16 to other parts of the integrated circuit, such as memory and controller circuits not shown in the drawing.

The operation of this random number generator will be explained with reference to Figs. 1 and 2.

When the integrated circuit is powered up, the counters 5 and 6 are reset to zero, the read signal is reset to the low (inactive) state and power is supplied to the oscillators 1 and 2, which begin generating clock pulses CP1 and CP2. Since the read signal is low, its inverse is high, so the clock pulses CP1 and CP2 are passed unchanged through the AND gates 3 and 4 to the counters 5 and 6 which begin counting them.

With reference to Fig. 2, the oscillators 1 and 2 may run at different rates. For example, oscillator 1 may run faster than oscillator 2, as illustrated at the top of Fig. 2, causing counter 5 to count faster than counter 6. Even if the oscillators 1 and 2 run at substantially the same rate, due to natural differences between component characteristics they will not run at exactly the same rate, nor will they run with perfect regularity, so they will quickly get out of step; hence the contents of the counters 5 and 6 will quickly become mutually unrelated.

When a random number is required, the read signal is driven high for an interval T1 in Fig. 2. During this interval the inverse of the read signal is low, so the outputs of the AND gates 3 and 4 remain low and the counters 5 and 6 stop counting. In addition, the output enable inputs of the counters 5 and 6 are high, so the read-out control circuits 7 and 8 output the counter contents Q1 to Q16 to the system bus 9. Since the counters 5 and 6 operate independently of each other and of the system clock, the value output from Q1 to Q16 is in effect a random number.

When the read signal is driven low again, the outputs Q1 to Q16 go to the high-impedance state and the counters 5 and 6 resume counting. When another random number is required, after the interval T2 in Fig. 2, the read signal again goes high, the counters 5 and 6 again stop, and their contents Q1 to Q16 are again output to the system bus. This output continues for the interval T3 during which the read signal is high.

If the interval T2 is sufficiently long, due to the independent counting rates of the counters 5 and 6 there will be no discernible relation between the first random number output during the interval T1 and the second random number output during the interval T3; the numbers, that is, will indeed be random. By continuing in the same way, a non-repeating series comprising any necessary number of random numbers can be generated.

To give the counters adequate time to get out of step, the minimum interval T2 between successive random numbers should preferably be an order of magnitude larger than the time required by the counters 5 and 6 to complete one counting cycle. In Fig. 1, the counters are eight-bit counters so a complete counting cycle comprises values from 0 to 255. If the intervals t1 and t2 between successive clock pulses CP1 and CP2 are on the order of 200ns, for example, a complete counting cycle takes approximately 256 x 200ns = 51.2μ s, so random numbers can be generated at intervals of about 0.5ms, which is much faster than in the prior art.

Furthermore, the circuitry required to generate the random numbers is extremely simple, comprising only a pair of oscillators, a pair of AND gates, and a pair of counters. This random number generator can accordingly be used as part of an integrated circuit without taking up excessive space.

If the counters 5 and 6 are not initialized to zero but have unpredictable values at power-up, the structure of the random generator can be further simplified by using just one oscillator. Such a random number generator will be described next with reference to Fig. 3.

The random number generator in Fig. 3 comprises the same oscillator 1, AND gate 3, and counters 5 and 6 as the random number generator in Fig. 1, but the counters 5 and 6 have unpredictable contents at power-up. The output of the AND gate 3 is connected to the clock terminals of both the counters 5 and 6. The operation of this random number generator is similar to the operation of the random number generator in Fig. 1, except that both counters 5 and 6 count clock pulses CP1 from the oscillator 1. Both counters thus count at the same rate, but since their contents are unpredictable at power-up and hence unrelated to begin with, the outputs Q1 to Q16 can again be used as random numbers.

The scope of this invention is not limited to the structures shown in the drawings, but includes various modifications and variations that will be apparent to one skilled in the art. In particular, the random number generator may have more than two counters, and the counters need not be eight-bit counters. Thirty-two bit random numbers, for example, can be generated using four eight-bit counters, or two sixteen-bit counters. When more than two counters are used, each counter can have its own oscillator as in Fig. 1, or if the counters are not initialized at power-up, they may share the same oscillator as in Fig. 2. The counters may be up-counters or

down-counters, or a mixture of both types.

The read-out means need not be structured as in Figs. 1 and 3; for example, it may comprise a circuit for capturing the counter contents into a register, making it unnecessary to stop the counters during random number output.

Claims

1. A data processing integrated circuit comprising data processing circuitry including a system bus (9) and a system clock, and a random number generator, wherein the random number generator comprises oscillator means (1,2) arranged to produce clock pulse signals (CP1, CP2) independent of the system clock, a plurality of counters (5,6) arranged to generate numbers by counting the clock pulse signals (CP1, CP2) end read out means responsive to a read signal (RD) from the processing circuitry to apply the counter contents directly to the system bus (9).

2. An integrated circuit according to claim 1, wherein the oscillator means (1,2) comprises a plurality of independent oscillators (1,2).

3. An integrated circuit according to claim 1 or 2, wherein the random number generator further comprises an AND gate (3,4), connected between said oscillator means (1,2) and said counter (5,6) for gating the said clock pulse signals (CP1,CP2) in response to the read signal (RD), and a read-out control circuit (7,8) disposed in each of the counters (5,6) for outputting the contents of the respective counters (5,6) in response to the read signal (RD).

4. An integrated circuit according to claim 1, 2 or 3, including read-out means for causing the counters (5,6) to stop counting while their contents are applied to the system bus (9).

Patentansprüche

1. Integrierte Datenverarbeitungsschaltung, die eine Datenverarbeitungs-Schaltungsanordnung mit einem Systembus (9) und einem Systemtakt sowie einen Zufallszahlen-Generator aufweist, wobei der Zufallszahlen-Generator folgendes aufweist: eine Oszillatoreinrichtung (1, 2), die dazu dient, vom Systemtakt unabhängige Taktimpulssignale (CP1, CP2) zu erzeugen, eine Mehrzahl von Zählern (5, 6), die dazu dienen, durch Zählen der Taktimpulssignale (CP1, CP2) Zahlen zu erzeugen, und eine Auslese-Einrichtung, die auf ein Lesesignal (RD) von der Datenverarbeitungs-Schaltungsanordnung anspricht, um die Inhalte der Zähler dem Systembus (9) direkt zuzuführen.

2. Integrierte Schaltung nach Anspruch 1, bei der die Oszillatoreinrichtung (1, 2) eine Mehrzahl unabhängiger Oszillatoren (1, 2) aufweist.

3. Integrierte Schaltung nach Anspruch 1 oder 2, bei der der Zufallszahlen-Generator weiterhin folgendes aufweist: ein UND-Glied (3, 4), das zwischen die Oszillatoreinrichtung (1, 2) und den Zähler (5, 6) geschaltet ist, um die Taktimpulssignale (CP1, CP2) in Reaktion auf das Lesesignal (RD) durchzuschalten, und eine Auslese-Steuerschaltung (7, 8), die in jedem Zähler (5, 6) angeordnet ist, um die Inhalte der entsprechenden Zähler (5, 6) in Reaktion auf das Lesesignal (RD) auszugeben.

4. Integrierte Schaltung nach Anspruch 1, 2 oder 3, die eine Auslese-Einrichtung aufweist, um zu bewirken, daß die Zähler (5, 6) mit dem Zählen aufzuhören, während ihre Inhalte dem Systembus (9) zugeführt werden.

Revendications

1. Circuit intégré pour le traitement de données, comportant des circuits de traitement de données incluant un bus système (9) et une horloge système, et un générateur de nombres aléatoires, dans lequel le générateur de nombres aléatoires comporte des moyens (1, 2) formant oscillateurs agencés pour produire des signaux d'impulsion d'horloge (CP1, CP2) indépendants de l'horloge système, plusieurs compteurs (5, 6) agencés pour engendrer des nombres en décomptant les signaux d'impulsion d'horloge (CP1, CP2) et des moyens de lecture réagissant à un signal de lecture (RD) provenant des circuits de traitement pour envoyer le contenu du compteur directement vers le bus système (9).

2. Circuit intégré selon la revendication 1, dans lequel les moyens (1, 2) formant oscillateurs comportent plusieurs oscillateurs indépendants (1, 2).

3. Circuit intégré selon la revendication 1 ou 2, dans lequel le générateur de nombres aléatoires comporte, en outre, une porte ET (3, 4) reliée entre lesdits moyens (1, 2) formant oscillateurs et lesdits compteurs (5, 6) pour transmettre lesdits signaux d'impulsion d'horloge (CP1, CP2) en réponse au signal de lecture (RD), et un circuit de commande de lecture (7, 8) disposé dans chacun des compteurs (5, 6) pour envoyer le contenu des compteurs respectifs (5, 6) en réponse au signal de lecture (RD).

4. Circuit intégré selon la revendication 1, 2 ou 3, com-

portant des moyens de lecture pour amener les compteurs (5, 6) à interrompre leur comptage pendant que leurs contenus sont envoyés vers le bus système (9).

FIG. 1

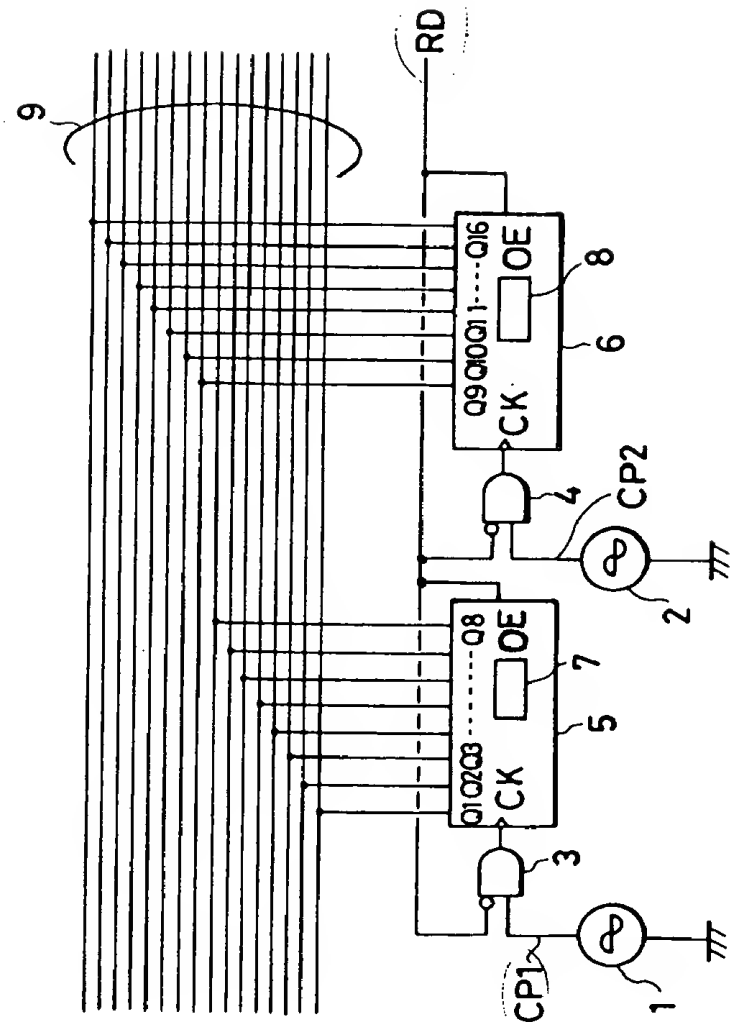

FIG. 2

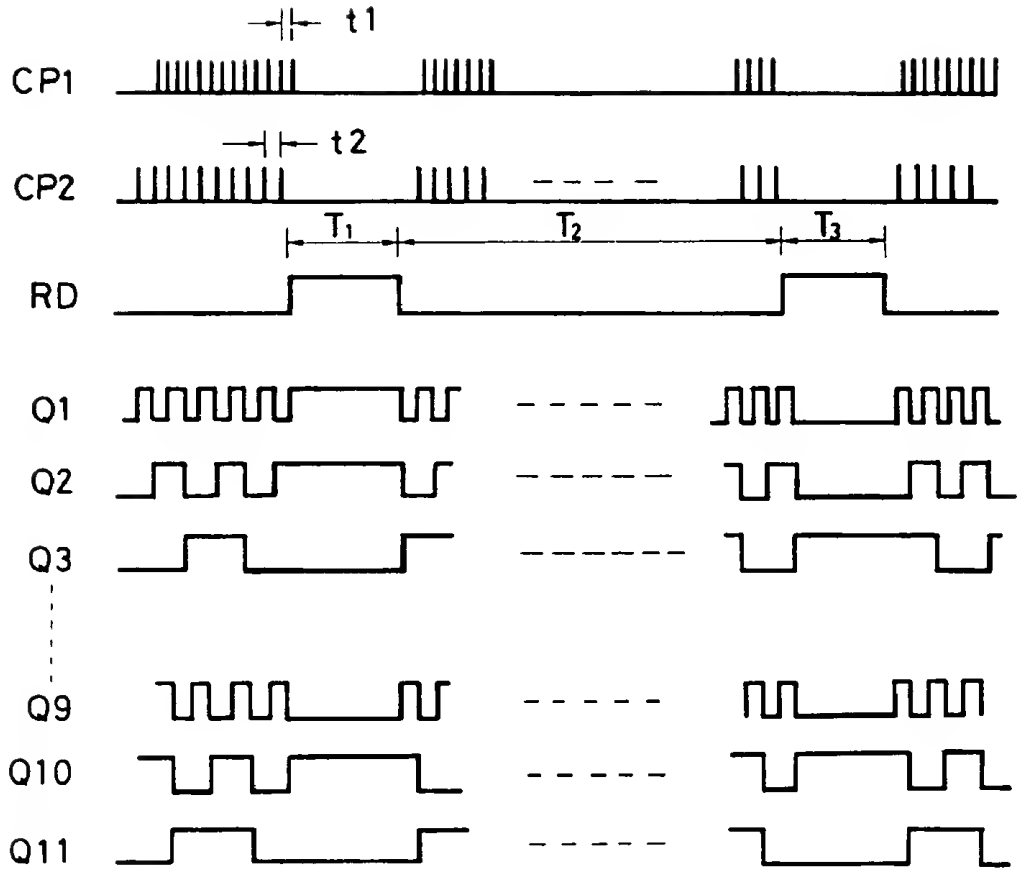

FIG. 3